UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/035,311	01/04/2002	Takehisa Kato	P 290460 T2TYA-97S0351-1C	2529

7590 02/13/2006

Pillsbury Winthrop LLP
Intellectual Property Group
1600 Tysons Boulevard
McLean, VA 22102

EXAMINER	
CALLAHAN, PAUL E	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 02/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/035,311	KATO ET AL.	
	Examiner	Art Unit	
	Paul Callahan	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 October 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *25,29,32-36,38 and 41-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *29,32-36,38 and 41-47* is/are allowed.

6)☒ Claim(s) *25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (~~PTO-1449 or PTO/SB/08~~) ~~Paper No(s)/Mail Date~~ . PC
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-47 were pending in this application at the time of the previous Office Action. By the amendment filed 10-3-2005, claims 1-24, 26-28, 30-31, 37, 39, and 40 are cancelled. Therefore claims 25, 29, 32-36, 38 and 41-47 remain pending and have been examined.

Response to Arguments

2. Applicant's arguments, presented with the amendment filed 10-3-2005, with respect to claims 1-47 have been fully considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claim 25 is rejected under 35 U.S.C. 102(b) as being clearly anticipated by Smith et al. US 6,823,070.

Smith teaches an enciphering method (abstract, col. 1 lines 62-67), comprising: keeping a plurality of second keys (col. 6 lines 33-40), enciphering data with a first key (col. 1 lines 62-67, col. 4 lines 10-35): enciphering said first key with a p number of

second keys, where p is an integer greater than or equal to two of the kept plurality of second keys to obtain a p number of enciphered first keys respectively (col. 4 lines 33-54, col. 6 lines 29-67, col. 7 lines 1-67); and selecting part of said plurality of second keys as said p number of second keys for use in enciphering said first key in a case where part of said plurality of second keys has been broken (col. 4 lines 33-54, col. 6 lines 29-67, col. 7 lines 1-67: the principal escrow agent only requires a subset of the mask-encrypted keys to reconstruct the key).

Allowable Subject Matter

5. Claims 29, 32-36, 38 and 41-47 are allowed.

6. The following is an examiner's statement of reasons for allowance:

The closest prior art in the field, Haas US 5,719,938, and Smith 6,823, 070, do not teach the features found in the independent claims of:

As per claims 29 and 38: enciphering data with a first key, and then enciphering that first key with a P number of second keys, where P is an integer greater than or equal to 2, and as a result of this enciphering the first key obtaining a P number of enciphered first keys, and selecting a part of this plurality of second keys as the number of P second keys used for enciphering the first key in the event where a part of said plurality of second keys has been broken. The claims are distinguished from the teachings Smith in particular since Smith teaches an escrow system where the plurality

of second keys are not stored in a common location until the time to recover the p number of enciphered first keys,

As per claims 32, 34, and 35: recording at least a part of a number P of second keys, where p is an integer greater than or equal to two, in a secret area in a deciphering device; inputting first enciphered data obtained by enciphering data with a first key and second information composed of a p number of enciphered first keys obtained by enciphering the first key with the P number of second keys, respectively; and then deciphering at least one of the P number of enciphered first keys using the recorded P number of second keys to obtain said first key; and confirming that the obtained first key is correct; and then deciphering the enciphered data using the obtained first key after the confirmation step. The claims are distinguished from the teachings Smith in particular since Smith teaches an escrow system where the plurality of second keys are not stored in a common location until the master seeks to recover the p number of enciphered first keys,

As for claim 36: a key control method wherein a first caretaker takes custody of a plurality of second keys; a second caretaker takes custody of first information composed of enciphered data obtained by enciphering data with a first key and second information composed of a P number of enciphered first keys, where P is an integer greater than or equal to two, obtained by enciphering said first key with a P number of second keys of said plurality of second keys, respectively, and a third caretaker that takes custody of at

least part of said plurality of second keys, said at least part of said plurality of second keys being recorded in a secret area of a device provided by the third caretaker. The claims may be distinguished in particular from Smith since the claims do not teach the plurality p of second keys being stored at separate locations as with the dependent masks of Smith.

As for claim 41: storing a plurality of master keys, allocating at least part of the plurality of master keys to a player maker; receiving a session key supplied from a disk maker; selecting part of the plurality of master keys for use in enciphering the session key in a case where part of the plurality of master keys has been broken; enciphering the received session key with a selected part of the plurality of master keys to produce a plurality of enciphered session keys, and supplying the produced plurality of enciphered session keys to said disk maker. The claims may be distinguished in particular from Smith since the claims do not teach the plurality p of second keys being stored at separate locations as with the dependent masks of Smith,

As for claim 42: storing a plurality of second keys, enciphering data with a first key; enciphering said first key with a P number of the second keys where P is an integer greater than or equal to two, thereby obtaining a P number of enciphered first keys, and then enciphering said first key with the first key itself. The claim may be distinguished from Smith in particular since Smith does not teach the feature of the first key being encrypted by itself,

As for claims 43, 46 and 47: a key control method applied to a key control organization, a disk maker, and a player maker. The claims may be distinguished from the teachings of Smith in particular since smith does not teach the features found in the claim of a player device provided a player maker with one or more master keys, and a disk supplied by a disk maker, and a third information obtained by enciphering a session key with itself.

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is: (571) 273-8300.

2-1-06

Paul Callahan

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER